Public Knowledge

April 11, 2018

The Honorable Greg Walden
Chairman
House Energy & Commerce Committee
2185 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member
House Energy & Commerce Committee
237 Cannon House Office Building
Washington, DC 20515

Dear Chairman Walden and Ranking Member Pallone,

On behalf of Public Knowledge, a public interest advocacy organization dedicated to promoting freedom of expression, an open internet, and access to affordable communications tools and creative works, we applaud the House Energy & Commerce Committee for holding a hearing on "Facebook: Transparency and Use of Consumer Data." We appreciate the opportunity to submit this letter for the record.

The Facebook disclosures over the last several weeks have been unrelenting. First, we learned that an app developer, Aleksandr Kogan, funneled personal information about at least 87 million Facebook users to Cambridge Analytica, a firm that purported to engage in "psychographics" to influence voters on behalf of the Trump campaign. Gallingly, as was Facebook's practice for all apps at that time, when users connected Kogan's app to their Facebook accounts, the app scooped up not only the users' personal information, but also their friends' information – without any notice to the friends or opportunity for the friends to consent. We then learned that Facebook had been collecting Android users' SMS and call histories. While Android users may have technically consented to that data collection, the outrage this news provoked strongly suggests that the notice Facebook provided about the practice was insufficient to permit users to understand precisely to what they were consenting. Last week, we learned that "malicious actors" used Facebook's search tools to build profiles of individuals whose e-mail addresses and phone numbers had been stolen in data breaches over the years and posted on the dark web. These profiles enabled identity theft.

But Facebook is hardly unique. In the twenty-first century, it is impossible to meaningfully participate in society without sharing our personal information with third parties. We increasingly live our lives online. We turn to platforms and companies to access education, health care, employment, the news, and emergency communications. We shop online. When we seek to rent a new apartment, buy a home, open a credit card, or, sometimes, apply for a job, someone checks our credit scores through companies on the internet. These third party companies and platforms should have commensurate obligations to protect our personal information, and those obligations must have the force of law. Unfortunately, it has become increasingly clear that too many third parties fail to live up to this responsibility. Rather, unauthorized access to personal data has run rampant – whether it is in the form of Cambridge Analytica, where authorized access to data was misused and shared in ways that exceeded authorization, or in the form of a data breach, where information was accessed in an unauthorized way. Just since the Cambridge Analytica news broke, consumers have learned of data breaches at Orbitz, Under Armour, Lord and Taylor, Saks Fifth Avenue, Saks Off Fifth, Panera Bread, Sears Holding Corp., and Delta Airlines.

We have also learned about purportedly authorized access to data that many consumers find unsavory and would likely not consent to, if they were clearly and fully informed of the nature of the transaction. For example, last week, we learned that Grindr has been sharing its users' HIV status with two other companies, Apptimize and Localystics. This sharing is almost certainly disclosed in Grindr's terms of service, but it is well known that few people read terms of service, and there is good reason to believe that had Grindr been upfront about this data sharing practices, few of its users would have agreed to it.

The industry has long insisted that it can regulate itself. However, the deluge of data breaches and unauthorized and unsavory use of consumer data makes clear that self-regulation is insufficient. Indeed, Facebook was already under a consent decree with the Federal Trade Commission (FTC), and yet it still failed to protect its users' personal information.

This hearing is a good start to begin addressing corporate collection and use of user data in the modern economy. But, a hearing alone is not enough. We hope that the Committee will use this hearing to build the record for strong, comprehensive privacy legislation. Here are three elements that any privacy legislation should include:

**Notice and Consent**

Until the digital age, individual ownership and control of one's own personal information was the basis for privacy law in the United States.[1] We should return to this principle. While we cannot avoid sharing information with some third parties, we can have greater control over that information. At a minimum, consumers should have a right to know a) what information is being collected and retained about them; b) how long that information is being retained; c) for what purposes that information is being retained; d) whether the retained information is identifiable, pseudo-anonymized, or anonymized; e) whether and how that information is being used; f) with whom that information is being shared; g) for what purposes that information is being shared; h) under what rubric that information is being shared (for free, in exchange for compensation, subject to a probable cause warrant, etc.); and (i) whether such information is being protected with industry recognized best practices.

It is imperative that this notice be meaningful and effective, which means that it cannot be buried in the fine print of a lengthy privacy policy or terms of service agreement. Consumers and companies know that consumers do not typically read privacy policies or terms of service agreements. Indeed, researchers at Carnegie Mellon estimate that it would take seventy-six work days for an individual to read all of the privacy policies she encounters in a year.[2] Companies take advantage of this common knowledge to bury provisions that they know consumers are unlikely to agree to in the fine print of these agreements. While courts have found these agreements to be binding contract, there is no reason that Congress cannot undo this presumption and insist that notice be provided in a way that consumers can quickly read and understand.

---

[1] HAROLD FELD, PRINCIPLES FOR PRIVACY LEGISLATION: PUTTING PEOPLE BACK IN CONTROL OF THEIR INFORMATION 19 – 20 (Public Knowledge, 2017).

[2] Alexis C. Madrigal, *Reading the Privacy Policies you Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, Mar. 1, 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

Moreover, notice alone is insufficient. Consumers must also have meaningful opportunities to freely and affirmatively consent to data collection, retention, and sharing. And, that consent should be as granular as possible. For example, a user should be able to consent for her data to be used for research purposes, but not for targeted advertising – or vice-versa. As with notice, the consent must be real rather than implied in the fine print of a terms of service. Consumers must also have the ability to withdraw their consent if they no longer wish for a company to use and retain their personal data, and they should be able to port their data in a machine-readable format to another service, if they so desire. In addition, service should not be contingent on the sharing of data that is not necessary to render the service.[3]

The General Data Protection Regulation, which goes into effect in Europe in May, will require some kinds of granular notice and consent, so companies already have to figure out how to offer their users opportunities for meaningful consent. There is no reason for them not to offer the same opportunities for meaningful notice and consent in the United States.

**Security Standards**

Organizations that are stewards of our personal information should be expected to adhere to recognized best practices to secure the information. This is particularly true when an individual cannot avoid sharing the information without foregoing critical services or declining to participate in modern society.

Relatedly, organizations should be required to adhere to privacy by design and by default and to practice data minimization. The presumption should be that only data necessary for the requested transaction will be retained, absent explicit consumer consent. Organizations should be encouraged to employ encryption, pseudo-anonymization, and anonymization to protect consumers' private information, and security mechanisms should be regularly evaluated. Importantly, these evaluations must be publicly conducted, with the government acting as convener of any multi-stakeholder process. Facebook/Cambridge Analytica, as well as the cascade of recent data breaches, has demonstrated that industry cannot be trusted to police itself.

**Meaningful Recourse**

When there is unauthorized access to personal information, individuals must be made whole to the greatest extent possible. There are two major barriers to this. The first is the Federal Arbitration Act, which requires courts to honor the forced arbitration clauses in contracts, including forced arbitration clauses buried in the fine print of terms of service agreements. Forced arbitration clauses require consumers to settle any dispute they have with a company by arbitration rather than having their day in court – and often consumers do not even know an arbitration clause

[3] While it may be appropriate for a non-essential service like Facebook to charge users a fee in lieu of selling their data, *see* Alex Johnson and Erik Ortiz, *Without data-targeted ads, Facebook would look like a pay service, Sandberg says*, NBC NEWS, Apr. 5, 2018, https://www.nbcnews.com/tech/social-media/users-would-have-pay-opt-out-all-facebook-ads-sheryl-n863151, such an approach is unacceptable for services that are integral for participation in society. Individuals should be able to access health care, education, housing, and other essential services without compromising their personal information or having to pay extra for their fundamental right to privacy.

is in their contract until they go to sue. This presents three problems: 1) Arbitrators are often more sympathetic to large companies, who are repeat players in the arbitration system, than most juries would be. 2) Arbitration creates no legal precedent. 3) Frequently, it is not cost-effective for an individual to bring a claim against a large company by herself. The damages she could win likely would not exceed her legal costs. But, when customers can band together in a class action lawsuit, it becomes much more feasible to bring a case against a large company engaged in bad behavior. Forced arbitration clauses preclude class action. Congress should explicitly exempt cases addressing the failure to protect personal information from the Federal Arbitration Act to make sure consumers can have their day in court when their information is misused and their trust abused.

The other major barrier to meaningful recourse is the difficulty calculating the damages associated with unauthorized access to personal information. While one may be able to quantify her damages when her credit card information is breached or her identity is stolen, it is much harder to do so in a situation like Facebook/Cambridge Analytica. It is difficult to put a dollar amount on having one's privacy preferences ignored or her personal information revealed to third parties without her knowledge or consent. We instinctively know that there is harm in having one's personal data used for "psychographics" to influence her behavior in the voting booth, but that harm is difficult to quantify. Congress already uses liquidated damages in other situations when the damage is real, but hard to quantify. In fact, liquidated damages are already used to address other privacy harms. For example, the Cable Privacy Act provides for liquidated damages when cable companies impermissibly share or retain personally identifiable information.

While the FTC can step in when companies engage in unfair and deceptive practices, the FTC is likely to only intervene in the most egregious cases. Moreover, the FTC can only extract damages from companies once they have violated users' privacy once, entered into a consent decree with the Agency, and then violated the consent decree. That means a lot of consumers have to have their personal information abused before a company is held to account. Moreover, when the FTC is involved, any damages go to the government, not to making individuals whole.

We are not recommending that the FTC be taken out of the business of protecting consumers in the digital age, but merely suggesting that consumers should also have the opportunity to protect ourselves. Allowing private, class action lawsuits for liquidated damages when companies fail to safeguard private information will create the necessary incentives for companies to take appropriate precautions to protect the information they have been entrusted with. Companies, after all, understand the technology and the risks, and are in the best position to develop safeguards to protect consumers.

**Existing Laws and Legislation**

While we hope that Congress will use this hearing to build the record for comprehensive privacy legislation, we encourage Congress to enact legislation that is compatible with existing federal sector-specific privacy laws in communications, health care, finance, and other sectors, as well as with state and local privacy laws. While the federal government should set minimum standards of protection for all Americans, states have been in the vanguard of privacy protection and are much-needed "cops on the beat." Even if Congress were to dramatically expand the resources

available to federal privacy agencies, the federal government could not hope to provide adequate protection to consumers on its own. Rather, the states, as laboratories of democracy, should be empowered to innovate and provide greater privacy protections to their residents.

These sector-specific privacy laws and state privacy laws, as well as legislation, introduced in this Congress and in previous Congresses, addressing notice and consent, security requirements, data breaches, and/or forced arbitration may be good building blocks for comprehensive legislation. But, Congress must ensure that the bills are updated to address today's harms. For example, many of the bills that have been drafted narrowly define personal information to include identifiers like first and last name, social security numbers, bank account numbers, etc. These bills would not personal cover the personal information in question in Facebook/Cambridge Analytica – information like social media "likes" that is certainly useful for influencing an individual in the voting booth, as well as for more mundane marketing and advertising purposes, and that, when aggregated, may, in fact, be personally identifiable.

**Conclusion**

Again, we appreciate the opportunity to submit this letter for the record for the House Energy & Commerce Committee hearing on "Facebook: Transparency and Use of Consumer Data" We look forward to continuing the conversation and stand ready to assist interested Members in crafting consumer privacy protection legislation. If you have any questions or would like more information, please do not hesitate to reach out to me at abohm@publicknowledge.org.

Sincerely,

Allison S. Bohm
Policy Counsel
Public Knowledge

CC. Members of the House Energy & Commerce Committee